UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,426	02/28/2002	Lauri Paatero	944-005.5	6252

4955 7590 12/06/2005

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
MIZAN, SHAHIN	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/090,426	**Applicant(s)** PAATERO, LAURI	
	Examiner Shahin Mizan	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 February 2002.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-44 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-44 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 February 2002 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-44 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Doyle et al. (US Patent 6,968,453).

As per independent claim 1, Doyle et al. teaches a method to allow at least one party to perform at least one permitted activity with respect to a device, comprising the steps of:

embedding a role certificate in said device, wherein the role certificate identifies said at least one permitted activity and wherein the role certificate is generated by a Certification Authority (CA) *(note Fig. 1 and associated description in the specification – the secure storage 156 or the memory 154 can hold multitude of role certificates; also note column 9, line 54 – the reference is applicable to PKI and hence the CA; also note column 7, lines 13-17 - the certificate is usually generated by CA; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*;

embedding at least information regarding a public key in said device the public key corresponding to the private key used by the CA to sign the role certificate *(note Fig. 1 and associated description in the specification – the secure storage 156 or the memory 154 can hold multitude of role certificates; also note column 9, line 54 – the reference is applicable to PKI and hence the CA; also note column 8, lines 1-30; also note column 9, lines 46-67; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*; and

running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party if the role certificate is verified *(note Fig. 1 and associated description in the specification – the secure core 150 is capable of performing the function; also note column 5, lines 1-24; also note column 6, lines 28-37; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 2, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate includes information regarding a control security level for said device so that the device only allows said at least one permitted activity to be a type of action which is within the security level of the device as defined by the role certificate *(note Fig. 1 and associated description in the specification – the secure core 150 is capable of performing the function; also note column 5, lines 1-24; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 3, which is dependent on claim 2, Doyle et al. teaches a method as defined in claim 2, wherein the security level defined by the role certificate allows a type of software code to be downloaded, and/or installed, and/or run on said device by said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-24; also note column 7, lines 13-17 - the certificate is usually generated by CA; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 4, which is dependent on claim 3, Doyle et al. teaches a method as defined in claim 3, wherein the type of software code is from the group of types of software code consisting of test code, production code and special code *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 11, lines 8-40 - third party capability upgrading means described).*

As per claim 5, which is dependent on claim 4, Doyle et al. teaches a method as defined in claim 4, wherein the special code can be code linked to a specific at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 11, lines 8-40 - third party capability upgrading means described).*

As per claim 6, which is dependent on claim 3, Doyle et al. teaches a method as defined in claim 3, wherein the role certificate further contains information with regard to a specific party of said at least one party that can download, and/or install, and/or run said type of software code *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 7, lines 13-17; also note column 5, lines 41-44*

- a user profile may contain role information; also note column 11, lines 8-40 - third party capability upgrading means described).

As per claim 7, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate further contains information with regard to a specific party of said at least one party that can activate the at least one permitted activity within the device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 8, which is dependent on claim 7, Doyle et al. teaches a method as defined in claim 7, wherein said information with regard to a specific party is a hash of information identifying said specific party's public key, and wherein the device validates said specific party by receiving said information identifying said specific party's public key, and hashing this information and comparing the hash value to the hash value contained in the role certificate so that if the hash values are equal, then the specific party is permitted to activate the at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note Fig. 3 and associated description in the specification; also note column 6, lines 1-27; also note column 11, lines 8-40 - third party capability upgrading means described).*

As per claim 9, which is dependent on claim 7, Doyle et al. teaches a method as defined in claim 7, wherein said specific party is a group of entities *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements* *depicted in the diagram; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 10, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the embedding of the role certificate into the device is performed after the information regarding the public key of the CA is embedded into the device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 11, which is dependent on claim 10, Doyle et al. teaches a method as defined in claim 1, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof; also note column 11, line 5).*

As per claim 12, which is dependent on claim 11, Doyle et al. teaches a method as defined in claim 11, wherein the tamper resistant area of the device is a portion memory in the device such that any modification of information stored therein can be ascertained *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof memory; also note column 11, line 5).*

As per claim 13, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected storage can contain certificates that perform the function using the I/O port; also note column 7, lines 13-17 - the digital certificate may contain the stated information; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 14, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the CA is a root CA *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 9, lines 46-67; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 15, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the device is a wireless device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-31; also note column 2, lines 19-41).*

As per claim 16, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the CA is any entity other than said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note Fig. 4; multiple entity can connect via multiple I/O ports or via one port; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 17, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity *(note Fig. 1 and associated description in the* *specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17).*

As per claim 18, which is dependent on claim 17, Doyle et al. teaches a method as defined in claim 17, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17).*

As per claim 19, which is dependent on claim 1, Doyle et al. teaches a method as deemed in claim 1, wherein said information regarding the CA public key is a hash value of said CA public key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note Fig. 3).*

As per independent claim 20, Doyle et al. teaches a role certificate mechanism to permit at least one activity to be activated in a device, comprising:

memory within the device containing a role certificate, wherein the role certificate identifies said at least one activity, and further where the memory contains information regarding a first key corresponding to a second key used to sign the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram such as protected storage 156 that can hold certificate as well as keys; also note also note column 7, lines 13-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*; and

means for running the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device *(note Fig. 1 and associated description in the specification – the secure* *core 150 is capable of performing the function; also note column 5, lines 1-24; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 21, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein the memory has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof).*

As per claim 22, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein the role certificate further includes information regarding the identity of a third party, and wherein the means for verifying the role certificate includes means for reading said third party identity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof)*;

wherein the role certificate mechanism further comprises means for receiving information from a third party and comparing at least a portion of said received information with the read third party identity from said role certificate, and if the comparison is the same, allowing said third party to perform said at least one activity on said device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 1-16; also note column 6, lines 28-36; also note column 5, lines 25-31).*

As per claim 23, which is dependent on claim 22, Doyle et al. teaches a role certificate mechanism as defined in claim 22, wherein said device is a mobile phone *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-51; also note column 2, lines 19-41; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 24, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein said device is a mobile phone *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-51; also note column 2, lines 19-41; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 25, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein said information regarding the first key is a hash of said first key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note Fig. 3 and associated description in the specification).*

As per independent claim 26, Doyle et al. teaches an apparatus to allow at least one party to perform at least one permitted activity with respect to a device, comprising:

means for embedding a role certificate in said device, wherein the role certificate identifies said at least one permitted activity and wherein the role certificate is generated by a Certification Authority (CA) *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 3-5; also note column 6, lines 46-54; column 7, lines 13-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*;

means for embedding information regarding a public key in said device, the public key corresponding to the private key used by the CA to sign the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 47-52; also note column 9, lines 46-67; also note 18, lines 66-67 plus the first paragraph in column 19)*; and

means for running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 6, lines 28-37 – this technique can be utilized to perform the function; also note column 7, lines 1-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 27, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate includes information regarding a control security level for said device so that the means for running the device provides that the at least one permitted activity to only be a type of action which is within the security level of the device as defined by the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 41-44 – a user can be a third party that is allowed to performs a specific role after being authenticated; also note column 6, lines 13-17 - the means for performing the function is described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 28, which is dependent on claim 27, Doyle et al. teaches a apparatus as defined in claim 27, wherein the security level defined by the role certificate allows a type of software code to be downloaded to said device by said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 23, lines 5-67).*

As per claim 29, which is dependent on claim 28, Doyle et al. teaches an apparatus as defined in claim 28, wherein the type of software code is from the group of types of software code consisting of test code, production code and special code *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 23, lines 5-67).*

As per claim 30, which is dependent on claim 29, Doyle et al. teaches a apparatus as defined in claim 29, wherein the special code can be code linked to a specific at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 23, lines 5-67).*

As per claim 31, which is dependent on claim 29, Doyle et al. teaches an apparatus as defined in claim 29, wherein the role certificate further contains information with regard to a specific party of said at least one party that can download, and/or install, and/or run said type of software code. *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 23, lines 5-67)*

As per claim 32, which is dependent on claim 27, Doyle et al. teaches a apparatus as defined in claim 27, wherein the role certificate further contains information with regard to a specific party of said at least one party that can activate the at least one permitted activity within the device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - each certificate can have different role associated with it; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 33, which is dependent on claim 32, Doyle et al. teaches an apparatus as defined in claim 32, wherein said information with regard to a specific party is a hash of information identifying said specific party's public key, and wherein the device validates said specific party by receiving said information identifying said specific party's public key, and hashing this information and comparing the hash value to the hash value contained in the role certificate so that if the hash values are equal, then the specific party is permitted to activate the at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 6, lines 1-27; also note Fig. 3 - the technique can be used to perform the stated function).*

As per claim 34, which is dependent on claim 32, Doyle et al. teaches an apparatus as defined in claim 32, wherein said specific party is a group of entities *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 41-44 - users can be a grouped to formed a party).*

As per claim 35, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area *(note Fig. 1 and associated description* *in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 11, line 5 - security core is tamper proof).*

As per claim 36, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein said information regarding the CA public key is a hash of said CA public key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 6, lines 1-27 and Fig. 3 - the hash technique can be utilized to perform the stated function).*

As per claim 37, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - each certificate can allow different role to include debugging; also note column 5, lines 41-44 - a user can have the privilege to perform the stated function as well).*

As per claim 38, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the device is a wireless device *(note Fig. 1 and associated description in the specification – the diagram is applicable to cell phone; also note column 6, line 67; also note column 23, lines 5-14; also note column 1, line 39; also note column 3, lines 15-23).*

As per claim 39, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the* *diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function).*

As per claim 40, which is dependent on claim 39, Doyle et al. teaches an apparatus as defined in claim 39, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; also note column 8, lines 20-24; also note column 15, lines 6-15).*

As per independent claim 41, Doyle et al. teaches a method to allow at least one party to perform at least one permitted activity that is applicable to a plurality of devices, comprising the steps of:

embedding a role certificate applicable to the plurality of devices in an individual device, wherein the role certificate specifies said at least one permitted activity and wherein the role certificate is generated by a Certification Authority (CA) *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12)*;

embedding at least information regarding a public key applicable to the plurality of devices in said individual device, the public key corresponding to the private key used by the CA to sir the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12)*; and running the individual device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the individual device by said at least one party if the role certificate is verified *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12; also note column 6, lines 28-37).*

As per claim 42, which is dependent on claim 41, Doyle et al. teaches the method of claim 41, wherein said individual device is also embedded with at least one different role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12).*

As per claim 43, which is dependent on claim 42, Doyle et al. teaches method of claim 42, wherein one of the at least one different role certificate specifies at least a third party or a group or a device, and wherein the at least one permitted activity is not conducted if the one of the at least one different role certificate does not match said at least a third party or a group or a device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12; also note column 6, lines 28-37).*

As per independent claim 44, Doyle et al. teaches an apparatus to allow at least one party to perform at least one permitted activity that is applicable to a plurality of devices, comprising:

means for embedding a role certificate applicable to the plurality of devices in an individual device, wherein the role certificate specifies said at least one permitted activity and wherein the role certificate is generated by a Certification Authority (CA) *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67)*;

means for embedding information regarding a public key applicable to the plurality of devices in said individual device, the public key corresponding to the private key used by the CA to sir the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12)*; and

means for running the individual device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the individual device by said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12; also note column 6, lines 28-37).*

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ramasubramani et al. (US Patent No. 6,516,316) teaches a centralized certificate management system for two-way interactive communication devices in data networks.

Hind et al. (US Patent No. 6,772,331) teaches a method and apparatus for exclusively pairing wireless devices.

Kivimaki et al. (US Patent No. 6,785,816) teaches a system and method for secured configuration data for programmable logic devices.

Wheeler et al. (US Patent No. 6,892,302) teaches incorporating security certificate during manufacture of device generating digital signatures.

Ikonen et al. (US Patent No. 6,804,357) teaches a method and system for providing secure subscriber content data.

Nykanen et al. (US Patent No. 6,714,778) teaches context sensitive web services.

Inquiries

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahin Mizan whose telephone number is 571-272-0687. The examiner can normally be reached on M-F 8:30 a.m. - 5:00 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

	Shahin Mizan Examiner Art Unit 2132

sm
SM

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100